

Leah M. Beligan, Esq. (SBN 250834)  
[lmbeligan@bbclawyers.net](mailto:lmbeligan@bbclawyers.net)  
Jerusalem F. Beligan, Esq. (SBN 211258)  
[jbeligan@bbclawyers.net](mailto:jbeligan@bbclawyers.net)  
**BELIGAN LAW GROUP, LLP**  
19800 MacArthur Blvd., Ste. 300  
Newport Beach, CA 92612  
Telephone: (949) 224-3881

James L. Simon (*pro hac vice* forthcoming)  
[james@simonsayspay.com](mailto:james@simonsayspay.com)  
**SIMON LAW CO.**  
5000 Rockside Road  
Liberty Plaza – Suite 520  
Independence, OH 44131  
Telephone: (216) 816-8696

Michael L. Fradin (*pro hac vice* forthcoming)  
[mike@fradinlaw.com](mailto:mike@fradinlaw.com)  
**FRADIN LAW**  
8401 Crawford Ave., Ste. 104  
Skokie, IL 60076  
Telephone: (847) 986-5889

*Attorneys for Plaintiff and the Putative Classes*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

|   |   |                            |
|---|---|----------------------------|
| Jatinder Singh and Sandeep Singh, Individually<br>and on behalf of all others similarly situated, | ) | Case No. _____             |
|   | ) |                            |
| Plaintiffs,   | ) | <b>COMPLAINT</b>           |
|   | ) |                            |
| vs.   | ) | <b><u>CLASS ACTION</u></b> |
|   | ) |                            |
|   | ) |                            |
| Payward, Inc. d/b/a Kraken  | ) |                            |
|   | ) |                            |
| Defendant.  | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |
|   | ) |                            |

**CLASS ACTION COMPLAINT**

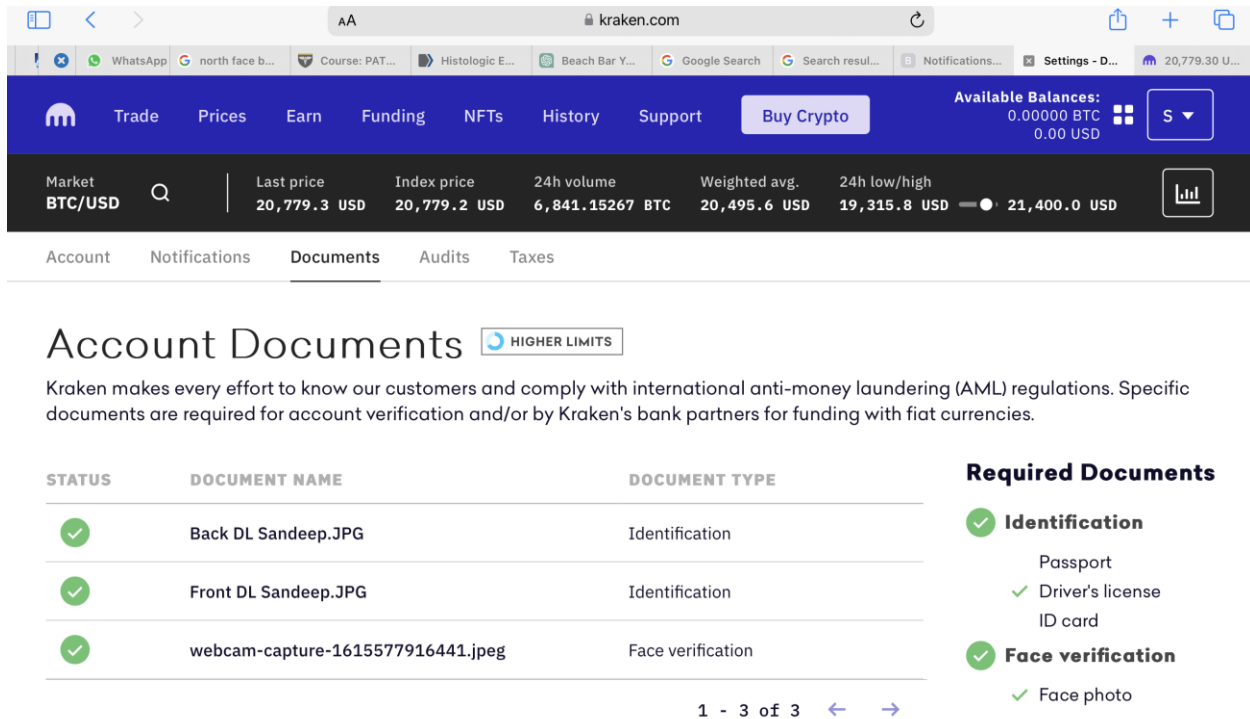
Now comes Plaintiffs, Jatinder Singh and Sandeep Singh (collectively “Plaintiffs”), on behalf of themselves and all other similarly situated, through Counsel, and pursuant to 735 ILCS §§ 5/2-801 and 2-802, and Fed. R. Civ. P. 23, against Defendant, Payward, Inc. (“Kraken” or “Defendant”), its subsidiaries and affiliates, to redress and curtail Defendant’s unlawful collections, obtainments, use, storage, and disclosure of Plaintiffs’ sensitive and proprietary biometric identifiers and/or biometric information (collectively referred to herein as “biometric data” and/or “biometrics”). Plaintiffs allege as follows upon personal knowledge as to themselves, their own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by their attorneys.

#### **NATURE OF THE ACTION**

1. Defendant, Payward, Inc. is a Delaware corporation which operates as an online, “app-based” platform wherein individuals can trade “crypto-currencies”, crypto-currency derivatives, and other virtual commodities.

2. Plaintiffs each opened a Kraken account within the five years immediately preceding the filing of this matter.

3. As part of signing up, and/or gaining access to their Kraken accounts, Plaintiffs were required to upload a picture of (1) a valid state-issued identification; and (2) a real time portrait of their face, i.e. a “selfie.”



The screenshot shows the Kraken.com website interface. At the top, there's a navigation bar with links like Trade, Prices, Earn, Funding, NFTs, History, Support, and a 'Buy Crypto' button. Below this is a market data section for BTC/USD. The main section is titled 'Account Documents' with a 'HIGHER LIMITS' badge. A paragraph explains that Kraken requires documents for account verification and AML compliance. Below this is a table of uploaded documents and a list of required documents.

| STATUS | DOCUMENT NAME                     | DOCUMENT TYPE     |
|--------|-----------------------------------|-------------------|
| ✓      | Back DL Sandeep.JPG               | Identification    |
| ✓      | Front DL Sandeep.JPG              | Identification    |
| ✓      | webcam-capture-1615577916441.jpeg | Face verification |

1 - 3 of 3

**Required Documents**

- ✓ **Identification**
  - Passport
  - ✓ Driver's license
  - ID card
- ✓ **Face verification**
  - ✓ Face photo

4. Kraken then scans the “selfie” photograph, creates a biometric template of the user’s face, and compares the user’s facial biometrics to the photograph on the identification document to confirm whether they match.

5. Kraken collects, stores, possesses, otherwise obtains, uses, and disseminates its users' biometric data to, amongst other things, further enhance Kraken and its online “app-based” platform.

6. Kraken wrongfully profits from the facial scans it has collected or otherwise obtained from its users.

7. Facial geometry scans are unique, permanent biometric identifiers associated with each user that cannot be changed or replaced if stolen or compromised. Kraken’s unlawful collection, obtainment, storage, and use of its users' biometric data exposes them to serious and

irreversible privacy risks. For example, if Kraken’s database containing facial geometry scans or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed, Kraken users have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

8. The Illinois legislature enacted BIPA to protect residents' privacy interests in their biometric data. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 963 (N.D. Ill. 2020), citing *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 432 Ill. Dec. 654, 129 N.E.3d 1197, 1199 (2019).

9. Courts analogize an individual's privacy interest in their unique biometric data to their interest in protecting their private domain from invasion, such as from trespass. *See Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020), as amended on denial of reh'g and reh'g *en banc*, (June 30, 2020) and opinion amended on denial of reh'g *en banc*, 2020 U.S. App. LEXIS 20468, 2020 WL 6534581 (7th Cir. 2020).

10. In recognition of these concerns over the security of individuals’ biometrics – particularly in the City of Chicago, which has been selected by major national corporations as a “pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias” (740 ILCS 14/5(b)) – the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like Kraken may not obtain and/or possess an individual’s biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used; (3) receives a written release from the person for the collection of his or her biometric identifiers or information; and (4) publishes

publicly-available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a)-(b).

11. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c). “For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” *Id.*

12. Specifically, upon information and belief, Kraken has created, collected, and stored thousands of “face templates” – highly detailed geometric maps of the face – from countless Illinois residents whose selfies and state-issued ID’s were collected by Kraken. Each face template that Kraken extracts is unique to a particular individual in the same way that a fingerprint or voiceprint uniquely identifies one, and only one, person.

13. Kraken is a “private entity” as that term is broadly defined by BIPA and Kraken is subject to all requirements of BIPA. *See* 740 ILCS § 14/10.

### **JURISDICTION AND VENUE**

14. This is a Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (740 ILCS 14/1 et seq.) brought pursuant to Fed. R. Civ. P. 23 seeking statutory and actual damages.

15. Venue is proper in this Court because a substantial amount of the acts and omissions giving rise to this Action occurred within this judicial district.

16. This Court has jurisdiction over this dispute pursuant to 28 U.S.C. § 1332 because Plaintiff and the proposed class members are all residents of Illinois, Kraken is domiciled within this judicial district and the amount in controversy exceeds \$75,000.

17. This Court has jurisdiction over this dispute pursuant to the Class Action Fairness Act (“CAFA”) because the prospective class includes over 100 people and the amount in controversy exceeds \$5,000,000.

18. At all relevant times, Plaintiffs are residents of the state of Illinois and the violations of BIPA as detailed herein occurred while Plaintiffs were located in Illinois.

19. At all relevant times, Kraken is incorporated under the laws and jurisdiction of Delaware, and Kraken’s principal place of business is located at 237 Kearny Street, Suite 102, San Francisco, California 94108.

#### **FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS**

20. Plaintiffs reallege and incorporate by reference all allegations in all preceding paragraphs.

21. Plaintiffs each opened Kraken accounts within the five years immediately preceding the filing of this action.

22. As part of signing up, and/or gaining access to their Kraken accounts, Plaintiffs were required to upload a picture of (1) a valid state-issued identification; and (2) a real time portrait of their face, i.e. a “selfie.”

The screenshot shows the Kraken.com website interface. At the top, there's a navigation bar with links like Trade, Prices, Earn, Funding, NFTs, History, Support, and a Buy Crypto button. Below this is a market data section for BTC/USD, showing last price, index price, 24h volume, weighted avg., and 24h low/high. The main content area is titled 'Account Documents' with a 'HIGHER LIMITS' button. It includes a paragraph about Kraken's AML regulations and a table of submitted documents. To the right, there's a 'Required Documents' section listing identification and face verification requirements.

| STATUS | DOCUMENT NAME                     | DOCUMENT TYPE     |
|--------|-----------------------------------|-------------------|
| ✓      | Back DL Sandeep.JPG               | Identification    |
| ✓      | Front DL Sandeep.JPG              | Identification    |
| ✓      | webcam-capture-1615577916441.jpeg | Face verification |

1 - 3 of 3

**Required Documents**

- ✓ **Identification**
  - Passport
  - ✓ Driver's license
  - ID card
- ✓ **Face verification**
  - ✓ Face photo

23. Kraken then scanned Plaintiffs' "selfie" photographs, creating a biometric template of the Plaintiffs' faces and biometric identifiers, and compared the Plaintiffs' biometric identifiers to the photographs on their state issued identification documents to confirm whether they match.

24. In other words, Kraken collected and retained biometric information for the purpose of verifying Plaintiffs' identities prior to opening a Kraken account in Plaintiffs' respective names.

25. At all relevant times, Kraken had no written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting or obtaining such biometric information has been satisfied or within 3 years of the individual's last interaction with Kraken, whichever occurs first. (*See* Kraken "Privacy Policy" attached hereto as Exhibit "A").

26. Ostensibly, the purpose Kraken's collection of Plaintiffs' biometric information was to verify Plaintiffs' identities prior to opening Kraken accounts in Plaintiffs' respective names.

27. As such, Plaintiffs' biometric information should have been permanently destroyed by Kraken following the opening of Plaintiffs' Kraken accounts.

28. However, Kraken failed to permanently destroy Plaintiffs' biometric information following the opening of Plaintiffs' Kraken accounts and instead retained Plaintiffs' biometric information.

29. As such, Kraken's retention of Plaintiffs' biometric information was unlawful and in violation of 740 ILCS § 14/15(a).

30. Kraken did not inform Plaintiffs in writing that Krake was collecting or storing their biometric information.

31. Instead, Kraken simply instructed Plaintiffs to upload their state issued identification forms and "selfie" photographs as part of the overall account opening process.

32. In fact, Kraken made no mention of biometric information, collection of biometric information, or storage of biometric information.

33. Moreover, Kraken did not inform Plaintiffs in writing of the specific purpose and length of term for which their biometric information was being collected, stored, and used.

34. Kraken collected, stored, and used Plaintiffs' biometric information without ever receiving a written release executed by Plaintiffs which would consent to or authorize Kraken to do the same.

35. Kraken has sold, leased, traded, or otherwise profited from Plaintiffs' biometric information. 740 ILCS § 14/15(c).



36. Kraken would not have opened an account in Plaintiffs' respective names had Plaintiffs not submitted their state issued identification, submitted their "selfie" photographs, allowed Kraken to collect their biometric information, and allowed Kraken to store or otherwise retain the same.

37. Plaintiffs were never offered any other means of verifying their identities in order to open a Kraken account.

38. As such, any and all revenue or profits which Kraken obtained as a result of Plaintiffs' patronage of Kraken was predicated upon Plaintiffs providing Kraken with their biometric information and Kraken's storage or retention of the same.

39. Additionally, Kraken disclosed, redisclosed, or otherwise disseminated a Plaintiffs' biometric information (1) without Plaintiffs' consent; (2) without Plaintiffs' authorization to complete a financial transaction requested or authorized by Plaintiffs; (3) without being required by State or federal law or municipal ordinance; or (4) without being required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

40. Kraken defines the Personal Information that it collects, stores and shares broadly as "any information relating to you, as an identified or **identifiable natural person**, including your name, an identification number, location data, or an **online identifier** or to one or more **factors specific** to the physical, economic, cultural or social **identity of you** as a natural person." (Ex. A at p. 2).

41. Kraken goes on to list multiple broad ways in which Kraken shares its users' confidential and personal information, including their biometric information as detailed herein:

## 7. Disclosure of your personal information

The Company will not disclose any of its clients' confidential information to a third party, except: (a) to the extent that it is required to do so pursuant to any applicable laws, rules or regulations; (b) if there is a duty to disclose; (c) if our legitimate business interests require disclosure; (d) in line with our Terms of Service; (e) at your request or with your consent or to those described in this Privacy Notice. The Company will endeavour to make such disclosures on a "need-to-know" basis, unless otherwise instructed by a regulatory authority. Under such circumstances, the Company will notify the third party regarding the confidential nature of any such information.

As part of using your personal information for the purposes set out above, the Company may disclose your personal information to the following:

Any members of the Company, which means that any of our affiliates and subsidiaries may receive such information;

Any of our service providers and business partners, for business purposes, such as specialist advisors who have been contracted to provide us with administrative, financial,

<https://www.kraken.com/legal/privacy>

---

3/16/23, 9:56 PM

Privacy Notice

legal, tax, compliance, insurance, IT, debt-recovery, analytics, research or other services;

If the Company discloses your personal information to service providers and business partners, in order to perform the services requested by clients, such providers and partners may store your personal information within their own systems in order to comply with their legal and other obligations.

We require that service providers and business partners who process personal information to acknowledge the confidentiality of this information, undertake to respect any client's right to privacy and comply with all relevant privacy and data protection laws and this Privacy Notice.

42. Kraken's collection and retention of biometric information as described herein is not unique to Plaintiff and is instead part Kraken's policy and procedures which Kraken applies to all of its users, including the Class Members.

### **RULE 23 CLASS DEFINITIONS AND ALLEGATIONS**

43. Plaintiffs reallege and incorporate by reference all allegations in all preceding paragraphs.

44. Plaintiffs bring Claims for Relief in violation of BIPA as a class action under Rule 23(a), (b)(2) and (b)(3). Plaintiffs brings these claims on behalf of themselves and all members of the following Rule 23 Class:

**All Illinois residents who had their biometric information collected by Kraken at any point in the five (5) years preceding the filing of this Complaint.**

45. In the alternative, and for the convenience of this Court and the parties, Plaintiffs may seek to certify other subclasses at the time the motion for class certification is filed.

46. **Numerosity (Rule 23(a)(1)).** The Class Members are so numerous that joinder of all members is impracticable. Plaintiffs are informed and believe that there are more than 1,000 people who satisfy the definition of the Class.

47. **Existence of Common Questions of Law and Fact (Rule 23(a)(2)).** Common questions of law and fact exist as to Plaintiffs and the Class Members including, but not limited to, the following:

a. Whether Kraken possessed Plaintiffs' and the Class Members' biometric identifiers or biometric information without first developing a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with Kraken, whichever occurs first.

b. Whether Kraken collected, captured, purchased, received through trade, or otherwise obtained Plaintiffs' and the Class Members' biometric identifiers or biometric

information, without first: (1) informing Plaintiffs and the Class Members in writing that a biometric identifier or biometric information is being collected or stored; (2) informing Plaintiffs and the Class Members in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used; and (3) receiving a written release executed by Plaintiffs and the Class Members

c. Whether Kraken sold, leased, traded, or otherwise profited from Plaintiffs' and the Class Members' biometric identifier or biometric information.

d. Whether Kraken disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class Members' biometric identifiers or biometric information (1) without Plaintiffs' and the Class Members' consent; (2) without Plaintiffs' and the Class Members' authorization to complete a financial transaction requested or authorized by Plaintiffs and the Class Members; (3) without being required by State or federal law or municipal ordinance; or (4) without being required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

e. The damages sustained and the proper monetary amounts recoverable by Plaintiffs and the Class Members.

48. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the Class Members' claims. Plaintiffs, like the Class Members, had their biometric identifiers and biometric information collected, retained or otherwise possessed by Kraken without Kraken's adherence to the requirements of BIPA as detailed herein.

49. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs have retained counsel competent and experienced in complex class actions.

50. **Injunctive and Declaratory Relief (Rule 23(b)(2)).** Class certification of the Rule 23 claims is appropriate under Rule 23(b)(2) because Kraken acted or refused to act on grounds generally applicable to the Class Members, making appropriate declaratory relief with respect to the Class Members as a whole.

51. **Predominance and Superiority of Class Action (Rule 23(b)(3)).** Class certification of the Rule 23 claims is also appropriate under Rule 23(b)(3) because questions of law and fact common to the Class Members predominate over questions affecting only individual members of the classes, and because a class action is superior to other available methods for the fair and efficient adjudication of this litigation. Kraken's common and uniform policies and practices illegally deprived Plaintiffs and the Class Members of the privacy protections which BIPA seeks to ensure; thus, making the question of liability and damages much more manageable and efficient to resolve in a class action, compared to hundreds of individual trials. The damages suffered by individual Class Members are small compared to the expense and burden of individual prosecution. In addition, class certification is superior because it will obviate the need for unduly duplicative litigation that might result in inconsistent judgments about Kraken's practices.

52. Plaintiffs intend to send notice to all Class Members to the extent required by Fed. R. Civ. P. 23.

**COUNT ONE: VIOLATION OF 740 ILCS § 14/15(a)**

53. Plaintiffs reallege and incorporate by reference all allegations in all preceding paragraphs.

54. A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the

initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines. 740 ILCS § 14/15(a).

55. Kraken scanned Plaintiffs' and the Class Members' "selfie" photographs, creating a biometric template of the Plaintiffs' and the Class Members' faces which qualifies as biometric information as defined by BIPA.

56. At all relevant times, Kraken had no written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting or obtaining such biometric information has been satisfied or within 3 years of the individual's last interaction with Kraken, whichever occurs first. (*See* Kraken's "Legal Privacy Notice" attached hereto as Exhibit "A").

57. Ostensibly, the purpose Kraken's collection of Plaintiffs' and the Class Members' biometric information was to verify Plaintiffs' identities prior to opening Kraken accounts in Plaintiffs' respective names.

58. As such, Plaintiffs' and the Class Members' biometric information should have been permanently destroyed by Kraken following the opening of Plaintiffs' Kraken accounts.

59. However, Kraken failed to permanently destroy Plaintiffs' and the Class Members' biometric identifiers and biometric information following the opening of Plaintiffs' and the Class Members' Kraken accounts and instead retained Plaintiffs' and the Class Members' biometric information.

60. As such, Kraken's retention of Plaintiffs' and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(a).

**COUNT TWO: VIOLATION OF 740 ILCS § 14/15(b)**

61. Plaintiffs realleges and incorporate by reference all allegations in all preceding paragraphs.

62. No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative. 740 ILCS § 14/15(b).

63. Kraken did not inform Plaintiffs and the Class Members in writing that Kraken was collecting or storing his biometric information.

64. Instead, Kraken simply instructed Plaintiffs and the Class Members to upload their state issued identification forms and "selfies" as part of the overall account opening process.

65. In fact, Kraken made no mention of biometric information, collection of biometric information, or storage of biometric information.

66. Moreover, Kraken did not inform Plaintiffs and the Class Members in writing of the specific purpose and length of term for which his biometric information as being collected, stored, and used.

67. Kraken collected, stored, and used Plaintiffs' and the Class Members' biometric information without ever receiving a written release executed by Plaintiffs and the Class Members which would consent to or authorize Kraken to do the same.

68. As such, Kraken's collection of Plaintiffs' and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(c).

**COUNT THREE: VIOLATION OF 740 ILCS § 14/15(c)**

69. Plaintiffs reallege and incorporate by reference all allegations in all preceding paragraphs.

70. No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information. 740 ILCS § 14/15(c).

71. Kraken has sold, leased, traded, or otherwise profited from Plaintiffs' and the Class Members' biometric information. 740 ILCS § 14/15(c).

72. Kraken would not have opened an account in Plaintiffs' or the Class Members' names had Plaintiffs and the Class Members not first submitted their state issued identifications, submitted their "selfies", allowed Kraken to collect their biometric information, and allowed Kraken to store or otherwise retain the same.

73. Plaintiffs and the Class Members were never offered any other means of verifying their identities in order to open Kraken accounts.

74. As such, any and all revenue or profits which Kraken obtained as a result of Plaintiffs' and Class Members' patronage of Kraken was predicated upon Plaintiffs and the Class Members providing Kraken with their biometric information and Kraken's storage or retention of the same.



75. While discovery will ascertain all of the ways in which Kraken has used Plaintiffs' and the Class Members' biometric information, Kraken admittedly uses Plaintiffs' and the Class Members' confidential and personal information, including their biometric information as described herein, for "business purposes", in furtherance of their "legitimate business interests", and for more specific profit-driven activities such as analytics and research. (*See* Ex. A at pp. 7-8).

76. Kraken's selling of, leasing of, trading of, or otherwise profitng from Plaintiffs' and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(c).

**COUNT FOUR: VIOLATION OF 740 ILCS § 14/15(d)**

77. Plaintiffs reallege and incorporate by reference all allegations in all preceding paragraphs.

78. No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. 740 ILCS § 14/15(d).

79. While discovery will ascertain all of the ways in which Kraken disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class Members' biometric information,

Kraken's Privacy Policy list multiple broad categories of third parties to which it discloses users' personal information, including biometric information:

## 7. Disclosure of your personal information

The Company will not disclose any of its clients' confidential information to a third party, except: (a) to the extent that it is required to do so pursuant to any applicable laws, rules or regulations; (b) if there is a duty to disclose; (c) if our legitimate business interests require disclosure; (d) in line with our Terms of Service; (e) at your request or with your consent or to those described in this Privacy Notice. The Company will endeavour to make such disclosures on a "need-to-know" basis, unless otherwise instructed by a regulatory authority. Under such circumstances, the Company will notify the third party regarding the confidential nature of any such information.

As part of using your personal information for the purposes set out above, the Company may disclose your personal information to the following:

Any members of the Company, which means that any of our affiliates and subsidiaries may receive such information;

Any of our service providers and business partners, for business purposes, such as specialist advisors who have been contracted to provide us with administrative, financial,

<https://www.kraken.com/legal/privacy>

3/16/23, 9:56 PM

Privacy Notice

legal, tax, compliance, insurance, IT, debt-recovery, analytics, research or other services;

If the Company discloses your personal information to service providers and business partners, in order to perform the services requested by clients, such providers and partners may store your personal information within their own systems in order to comply with their legal and other obligations.

We require that service providers and business partners who process personal information to acknowledge the confidentiality of this information, undertake to respect any client's right to privacy and comply with all relevant privacy and data protection laws and this Privacy Notice.

80. Kraken's disclosures, redisclosures, or otherwise disseminating of Plaintiffs' and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(d).

**WHEREFORE**, individually, and on behalf of the Class Members, the Plaintiffs pray for: (1) certification of this case as a class action pursuant to Fed. R. Civ. P. 23 appointing the undersigned counsel as class counsel; (2) a declaration that Kraken has violated BIPA, 740 ILCS 14/1 *et seq.*; (3) statutory damages of \$5,000.00 for the intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 per violation pursuant to 740 ILCS 14/20(1) in the event the court finds that Kraken's violations of BIPA were negligent; (4) reasonable attorneys' fees and costs and other litigation expense pursuant to 740 ILCS 14/20(3); (5) actual damages; and (6) for any other relief deemed appropriate in the premises.

**DEMAND FOR JURY TRIAL**

Plaintiffs and the Class members hereby demand a jury trial on all causes of action and claims with respect to which they each have a state and/or federal constitutional right to a jury trial.

Dated: March 27, 2023

Respectfully submitted,

**BELIGAN LAW GROUP, LLP**

By: /s/ Leah M. Beligan  
Leah M. Beligan, Esq. (SBN 250834)  
[lmbeligan@bbclawyers.net](mailto:lmbeligan@bbclawyers.net)  
Jerusalem F. Beligan, Esq. (SBN 211258)  
[jbeligan@bbclawyers.net](mailto:jbeligan@bbclawyers.net)  
19800 MacArthur Blvd., Ste. 300  
Newport Beach, CA 92612  
Telephone: (949) 224-3881

**FRADIN LAW**

s/ Michael L. Fradin

Michael L. Fradin, Esq. (pro hac vice forthcoming)

8 N. Court St. Suite 403

Athens, Ohio 45701

Telephone: 847-986-5889

Facsimile: 847-673-1228

Email: [mike@fradinlaw.com](mailto:mike@fradinlaw.com)

**SIMON LAW CO.**

By: /s/ James L. Simon

James L. Simon (pro hac vice forthcoming)

Simon Law Co.

5000 Rockside Road

Liberty Plaza – Suite 520

Independence, OH 44131

Telephone: (216) 816-8696

Email: [james@simonsayspay.com](mailto:james@simonsayspay.com)

# EXHIBIT A

## Legal

# Privacy Notice

*Last Updated: Oct 10, 2022*

## 1. Introduction

As part of our daily business operations, we collect personal information from our clients and prospective clients in order to provide them with our products and services, and ensure that we can meet their needs when providing these products and services, as well as when providing them with any respective information.

Your privacy is of utmost importance to us, and it is our policy to safeguard and respect the confidentiality of information and the privacy of individuals. This Privacy Notice sets out how Kraken API products and services provided by Payward Inc.; its affiliates and subsidiaries (collectively, the Payward Entities dba "Kraken", "the Company", "We", "Us", and the trading and direct sales services provided by Kraken (collectively the "Kraken Exchange" or "Exchange"), collects, uses and manages the personal information we receive from you, or a third party, in connection with our provision of services to you or which we collect from your use of our services and/or our website. The Privacy Notice also informs you of your rights with respect to the processing of your personal information.

Our Privacy Notice is reviewed regularly to ensure that any new obligations and technologies, as well as any changes to our business operations and practices are taken into consideration, as well as that it remains abreast of the changing regulatory environment. Any personal information we hold will be governed by our most recent Privacy Notice.

Please note that if you are an employee of the Company, a contractor to the Company or a third-party provider, your personal information will be used in connection with your employment contract or your contractual relationship, whichever applies.

This Privacy Notice applies to the processing activities performed by Kraken to the personal information of its clients and its potential clients and website visitors.

We may amend this Privacy Notice at any time by posting the amended version on this site including the effective date of the amended version. We will announce any material changes to this Privacy Notice on our website.

## 2. Definitions

2.1 As used herein, the following terms are defined as follows:

2.1.1 “Digital Asset” is a digital representation of value (also referred to as “cryptocurrency,” “virtual currency,” “digital currency,” “crypto token,” “crypto asset,” or “digital commodity”), such as bitcoin, XRP or ether, which is based on the cryptographic protocol of a computer network that may be (i) centralized or decentralized, (ii) closed or open-source, and (iii) used as a medium of exchange and/or store of value.

2.1.2 “Kraken Account” means a user-accessible account offered via the Kraken Exchange Services where Digital Assets are stored by Payward.

2.1.3 “Kraken Exchange Services” means Kraken-branded websites, applications, services, or tools operated by Payward group companies.

2.1.4 “We,” and “Us” refers to Kraken.

2.1.5 “Personal Information” or “Personal Data” or “your data” refers to any information relating to you, as an identified or identifiable natural person, including your name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of you as a natural person.

2.1.6 “VASP Services” means exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets, that is to say, conduct a transaction on behalf of another person that moves a virtual assets from one virtual asset address or account to another; and act as a custodian wallet provider.

## 3. Your Data Controller

Our products and services are provided through local operating entities that are subsidiaries of Payward Inc.

You are contracting with one Payward group company, as follows:

If you reside in Australia, you are contracting with Bit Trade Pty Limited, Unit 610, 478 George Street, Sydney, NSW 2000, Australia.

If you reside in Canada, you are contracting with Payward Canada Inc., 1100-1959 Upper Water Street, Halifax, NS B3J 3N2, Canada.

If you reside in the UK, you are contracting with Payward Ltd., 6th Floor, One London Wall, London, EC2Y 5EB.

If you reside in the United States, you are contracting with Payward Ventures Inc., 237 Kearny Street #102, San Francisco, CA 94108.

If you reside in Italy you are contracting with Payward Europe Solutions Limited, 70 Sir John Rogerson's Quay, Dublin 2, D02 R296, operating through its Italian Branch, Payward Europe Solutions Limited, Italian Branch, 21 Via San Marco, Milan, MI, 20121, Italy (for

VASP Services). For all other clients located in the European Economic Area you are contracting with Payward International Markets Limited, Trinity Chambers, PO BOX 4301, Road Town, Tortola, British Virgin Islands.

If you reside in the rest of the world (other than Japan, in which case, you have been provided with a separate privacy notice that is applicable to you), you are contracting with Payward Trading Ltd., c/o SHRM Trustees (BVI) Limited, Trinity Chambers, Ora et Labora Building, Road Town, Tortola, VG1110, British Virgin Islands.

If you are a client of Kraken Futures, you are contracting with either Payward Brokers Pte. Ltd., or Payward Global Trading Pte. Ltd., 8 Tomasello Boulevard, #15-04, Suntec Tower Three, Singapore 038988.

The Company you are contracting with is your Data Controller, and is responsible for the collection, use, disclosure, retention and protection of your personal information in accordance with our global privacy standards, this Privacy Notice, as well as any applicable national laws. The Company uses encryption to protect your information and store decryption keys in separate systems. We process and retain your personal information on our servers in multiple data center locations, including the European Union, Japan, Australia, the United Kingdom, the United States of America and elsewhere in the world.

## 4. How do we protect personal information?

The Company respects the privacy of any users who access its website, and it is therefore committed to taking all reasonable steps to safeguard any existing or prospective clients, applicants and website visitors.

The Company keeps any personal data of its clients and its potential clients in accordance with the applicable privacy and data protection laws and regulations.

We have the necessary and appropriate technical and organisational measures and procedures in place to ensure that your information remains secure at all times. We regularly train and raise awareness for all our employees to the importance of maintaining, safeguarding and respecting your personal information and privacy. We regard breaches of individuals' privacy very seriously and will impose appropriate disciplinary measures, including dismissal from employment. We have also appointed a Group Data Protection Officer, to ensure that our Company manages and processes your personal information in compliance with the applicable privacy and data protection laws and regulations, and in accordance with this Privacy Notice.

The personal information that you provide us with when applying to open an account, applying for a role within the Company, or when using our website, is classified as registered information, which is protected in several ways. You can access your registered information after logging in to your account by entering your username and the password that you have selected. It is your responsibility to make sure that your password is only known to you and not disclosed to anyone else. Registered information is securely stored in a safe location, and only authorised personnel have access to it via a username and password. All personal information is transferred to the Company over a secure connection, and thus all reasonable measures are taken to prevent unauthorised parties from viewing any such information. Personal information provided to the Company that does not classify as registered information is also kept in a safe environment and accessible by authorised personnel only through username and password.



## 5. Information we may collect about you

In order to open an account with us, you must first complete and submit a “create account” form to us by completing the required information. By completing this form, you are requested to disclose personal information in order to enable the Company to assess your application and comply with the relevant laws (including their regulations).

The information that we collect from you is as follows:

Full name, residential address and contact details (e.g. email address, telephone number, fax etc.);

Date of birth, place of birth, gender, citizenship;

Bank account information, credit card details, including details about your source of funds, assets and liabilities, and OFAC information;

Trading account balances, trading activity, your inquiries and our responses;

Information on whether you hold a prominent public function (PEP);

Verification information, which includes information necessary to verify your identity such as a passport, driver's licence or Government-issued identity card);

Other Personal Information or commercial and/or identification information – Whatever information we, in our sole discretion, deem necessary to comply with our legal obligations under various anti-money laundering (AML) obligations, such as under the European Union's 4th AML Directive and the U.S. Bank Secrecy Act (BSA).

Information we collect about you automatically.

Browser Information – Information that is automatically collected via analytics systems providers from your browser, including your IP address and/or domain name and any external page that referred you to us, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system, and platform;

Log Information – Information that is generated by your use of Kraken Exchange Services that is automatically collected and stored in our server logs. This may include, but is not limited to, device-specific information, location information, system activity and any internal and external information related to pages that you visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our Website or App (including date and time; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page;

Information we receive about you from other sources.

We obtain information about you in a number of ways through your use of our services, including through any of our websites, the account opening process, webinar sign-up forms, event subscribing, news and updates subscribing, and from information provided in the course of on-going support service communications. We also receive information about you from third parties such as your payment providers and through publicly available sources. For example:

The banks you use to transfer money to us will provide us with your basic personal information, such as your name and address, as well as your financial information such as your bank account details;

Your business partners may provide us with your name and address, as well as financial information;

Advertising networks, analytics providers and search information providers may provide us with anonymized or de-identified information about you, such as confirming how you found our website;

Credit reference agencies do not provide us with any personal information about you, but may be used to corroborate the information you have provided to us.

## 6. Lawful basis for processing your personal information

We will process your personal information on the following bases and for the following purposes:

### **Performance of a contract**

We process personal data in order to provide our services and products, as well as information regarding our products and services based on the contractual relationship with our clients (i.e. so as to perform our contractual obligations). In addition, the processing of personal data takes place to enable the completion of our client on-boarding process.

In view of the above, we must verify your identity in order to accept you as our client and we will use your personal data in order to effectively manage your trading account with us. This may include third parties carrying out credit or identity checks on our behalf. The use of your personal information is necessary for us to know who you are, as we have a legal obligation to comply with "Know Your Customer" and customer due diligence regulatory obligations.

### **Compliance with a legal obligation**

There are a number of legal obligations imposed by relevant laws to which we are subject, as well as specific statutory requirements e.g. anti-money laundering laws, financial services laws, corporation laws, privacy laws and tax laws. There are also various supervisory authorities whose laws and regulations apply to us. Such obligations and requirements imposed on us necessary personal data processing activities for identity verification, payment processing, compliance with court orders, tax laws or other reporting obligations and anti-money laundering controls.

These obligations apply at various times, including client on-boarding, payments and systemic checks for risk management.

### **For the purpose of safeguarding legitimate interests**

We process personal data so as to safeguard the legitimate interests pursued by us or by a third party. A legitimate interest is when we have a business or commercial reason to use your information. Example of such processing activities include the following:

Initiating legal claims and preparing our defense in litigation procedures;

Means and processes we undertake to provide for the Company's IT and system security, preventing potential crime, asset security and access controls;

Measures for managing the business and for further developing products and services;

Sharing your data within the Payward Inc. group of companies for the purpose of updating and/or verifying your personal data in accordance with the relevant anti-money laundering compliance frameworks, and

Risk management.

**To provide you with products and services, or information about our products and services, and to review your ongoing needs.**

Once you successfully open an account with us, or subscribe to information, we must use your personal information to perform our services and comply with our obligations to you. It is also in our legitimate interests to try to ensure that we are providing the best products and services so we may periodically review your needs based on our assessment of your personal information to ensure that you are getting the benefit of the best possible products and services from us.

**To help us improve our products and services, including support services, and develop and market new products and services.**

We may, from time-to-time, use personal information provided by you through your use of the services and/or through client surveys to help us improve our products and services. It is in our legitimate interests to use your personal information in this way to try to ensure the highest standards when providing you with our products and services and to continue to be a market leader within the cryptocurrency financial service industry.

**To investigate or settle enquiries or disputes**

We may need to use personal information collected from you to investigate issues or to settle disputes with you because it is our legitimate interest to ensure that issues and disputes get investigated and resolved in a timely and efficient manner.

**To comply with applicable laws, subpoenas, court orders, other judicial process, or the requirements of any applicable regulatory authorities**

We may need to use your personal information to comply with any applicable laws and regulations, subpoenas, court orders or other judicial processes, or requirements of any applicable regulatory authority. We do this not only to comply with our legal obligations but because it may also be in our legitimate interest to do so.

**To send you surveys**

From time to time, we may send you surveys as part of our client feedback process. It is in our legitimate interest to ask for such feedback to try to ensure that we provide our products and services at the highest standard. However, we may from time to time also ask you to participate in other surveys and if you agree to participate in such surveys we rely on your consent to use the personal information we collect as part of such surveys. All responses to any survey we send out whether for client feedback or otherwise will be aggregated and depersonalised before the results are published and shared.

**Data analysis**

Our website pages and emails may contain web beacons or pixel tags or any other similar types of data analysis tools that allow us to track receipt of correspondence and count the number of users that have visited our webpage or opened our correspondence. We may aggregate your personal information with the personal information of our other clients on

an anonymous basis (that is, with your personal identifiers removed), so that more rigorous statistical analysis of general patterns may lead us to providing better products and services.

If your personal information is completely anonymised, we do not require a legal basis as the information will no longer constitute personal information. If your personal information is not in an anonymised form, it is in our legitimate interest to continually evaluate that personal information to ensure that the products and services we provide are relevant to the market.

### Marketing purposes

We may use your personal information to send you marketing communications by email or other agreed forms (including social media campaigns), to ensure you are always kept up-to-date with our latest products and services. If we send you marketing communications we will do so based on your consent and registered marketing preferences.

### Internal business purposes and record keeping

We may need to process your personal information for internal business and research purposes as well as for record keeping purposes. Such processing is in our own legitimate interests and is required in order to comply with our legal obligations. This may include any communications that we have with you in relation to the products and services we provide to you and our relationship with you. We will also keep records to ensure that you comply with your contractual obligations pursuant to the agreement ("Terms of Service") governing our relationship with you.

### Legal Notifications

Often the law requires us to advise you of certain changes to products or services or laws. We may need to inform you of changes to the terms or the features of our products or services. We need to process your personal information to send you these legal notifications. You will continue to receive this information from us even if you choose not to receive direct marketing information from us.

## 7. Disclosure of your personal information

The Company will not disclose any of its clients' confidential information to a third party, except: (a) to the extent that it is required to do so pursuant to any applicable laws, rules or regulations; (b) if there is a duty to disclose; (c) if our legitimate business interests require disclosure; (d) in line with our Terms of Service; (e) at your request or with your consent or to those described in this Privacy Notice. The Company will endeavour to make such disclosures on a "need-to-know" basis, unless otherwise instructed by a regulatory authority. Under such circumstances, the Company will notify the third party regarding the confidential nature of any such information.

As part of using your personal information for the purposes set out above, the Company may disclose your personal information to the following:

Any members of the Company, which means that any of our affiliates and subsidiaries may receive such information;

Any of our service providers and business partners, for business purposes, such as specialist advisors who have been contracted to provide us with administrative, financial,

legal, tax, compliance, insurance, IT, debt-recovery, analytics, research or other services;

If the Company discloses your personal information to service providers and business partners, in order to perform the services requested by clients, such providers and partners may store your personal information within their own systems in order to comply with their legal and other obligations.

We require that service providers and business partners who process personal information to acknowledge the confidentiality of this information, undertake to respect any client's right to privacy and comply with all relevant privacy and data protection laws and this Privacy Notice.

## 8. Where we store your personal data

Our operations are supported by a network of computers, servers, and other infrastructure and information technology, including, but not limited to, third-party service providers. We and our third-party service providers and business partners store and process your personal data in the European Union, Japan, the United Kingdom, the United States of America and elsewhere in the world.

## 9. Transfers of personal information outside of the European Economic Area (EEA) and the United Kingdom (UK)

We may transfer your personal information outside the EEA and UK to other Company subsidiaries, service providers and business partners (i.e Data Processors) who are engaged on our behalf. To the extent that we transfer your personal information outside of the EEA and UK, we will ensure that the transfer is lawful and that Data Processors in third countries are obliged to comply with the European Union (EU) General Data Protection Act 2016 and the UK Data Protection Act 2018. If transfers of personal information are processed in the US, we may in some cases rely on standard contractual clauses.

## 10. Transfers of Personal Information outside of your country

By using our products and services, you consent to your Personal Data being transferred to other countries, including countries that have differing levels of privacy and data protection laws than your country. In all such transfers, we will protect your personal information as described in this Privacy Notice, and ensure that appropriate information sharing contractual agreements are in place.

## 11. Privacy when using digital assets and blockchains

Your funding of bitcoin, XRP, ether, and other Digital Assets, may be recorded on a public blockchain. Public blockchains are distributed ledgers, intended to immutably record transactions across wide networks of computer systems. Many blockchains are open to forensic analysis which can lead to deanonymization and the unintentional revelation of

private financial information, especially when blockchain data is combined with other data.

Because blockchains are decentralized or third-party networks which are not controlled or operated by Payward or its affiliates, we are not able to erase, modify, or alter personal data from such networks.

## 12. Data Retention

Safeguarding the privacy of your personal information is of utmost importance to us, whether you interact with us personally, by phone, by email, over the internet or any other electronic medium. We will hold personal information, for as long as we have a business relationship with you, in secure computer storage facilities, and we take the necessary measures to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

When we consider that personal information is no longer necessary for the purpose for which it was collected, we will remove any details that will identify you or we will securely destroy the records. However, we may need to maintain records for a significant period of time (after you cease being our client). For example, we are subject to certain anti-money laundering laws which require us to retain the following, for a period of 5 years after our business relationship with you has ended.

A copy of the records we used in order to comply with our client due diligence obligations;

Supporting evidence and records of transactions with you and your relationship with us.

Also, the personal information we hold in the form of a recorded information, by telephone, electronically or otherwise, will be held in line with local regulatory requirements (i.e. 5 years after our business relationship with you has ended or longer if you have legitimate interests (such as handling a dispute with you)). If you have opted out of receiving marketing communications we will hold your details on our suppression list so that we know you do not want to receive these communications.

We may keep your data for longer than 5 years if we cannot delete it for legal, regulatory, or technical reasons.

## 13. Cookies

When you use our products and services, we may make use of the standard practice of placing tiny data files called cookies, flash cookies, pixel tags, or other tracking tools (herein, "Cookies") on your computer or other devices used when engaging with us. We use Cookies to (i) help us recognize you as a customer, collect information about your use of our products and services, to better customize our services and content for you, and to collect information about your computer or other access devices to ensure our compliance with our BSA and AML obligations.

## 14. Your rights regarding your personal information

The rights that are available to you in relation to the personal information we hold about you are outlined below.

### **Information Access**

If you ask us, we will confirm whether we are processing your personal information and, if so, what information we process and, if requested, provide you with a copy of that information within 30 days from the date of your request.

### **Rectification**

It is important to us that your personal information is up to date. We will take all reasonable steps to make sure that your personal information remains accurate, complete and up-to-date. If the personal information we hold about you is inaccurate or incomplete, you are entitled to have it rectified. If we have disclosed your personal information to others, we will let them know about the rectification where possible. If you ask us, if possible and lawful to do so, we will also inform you with whom we have shared your personal information so that you can contact them directly.

You may inform us at any time that your personal details have changed by emailing us at support@kraken.com. The Company will change your personal information in accordance with your instructions. To proceed with such requests, in some cases we may need supporting documents from you as proof i.e. personal information that we are required to keep for regulatory or other legal purposes.

### **Erasure**

You can ask us to delete or remove your personal information in certain circumstances such as if we no longer need it, provided that we have no legal obligation to retain that data. Such requests will be subject to the contract that you have with us, and to any retention limits we are required to comply with in accordance with applicable laws and regulations. If we have disclosed your personal information to others, we will let them know about the erasure request where possible. If you ask us, if possible and lawful to do so, we will also inform you with whom we have shared your personal information so that you can contact them direct.

### **Processing restrictions**

You can ask us to block or suppress the processing of your personal information in certain circumstances such as if you contest the accuracy of that personal information or object to us processing it. It will not stop us from storing your personal information. We will inform you before we decide not to agree with any requested restriction. If we have disclosed your personal information to others, we will let them know about the restriction of processing if possible. If you ask us, if possible and lawful to do so, we will also inform with whom we have shared your personal information so that you can contact them direct.

### **Data portability**

In certain circumstances you might have the right, to obtain personal information you have provided us with (in a structured, commonly used and machine readable format) and to re-use it elsewhere or ask us to transfer this to a third party of your choice.

### **Objection**

You can ask us to stop processing your personal information, and we will do so, if we are:

Relying on our own or someone else's legitimate interests to process your personal information except if we can demonstrate compelling legal grounds for the processing;

Processing your personal information for direct marketing; or

Processing your personal information for research unless we reasonably believe such processing is necessary or prudent for the performance of a task carried out in the public interest (such as by a regulatory or enforcement agency).

#### **Automated decision-making and profiling**

If we have made a decision about you based solely on an automated process (e.g. through automatic profiling) that affects your ability to access our products and services or has another significant effect on you, you can request not to be subject to such a decision unless we can demonstrate to you that such decision is necessary for entering into, or the performance of, a contract between you and us. Even if a decision is necessary for entering into or performing a contract, you may contest the decision and require human intervention. We may not be able to offer our products or services to you, if we agree to such a request (i.e. end our relationship with you).

## **15. Changes to this Privacy Notice**

Our Privacy Notice is reviewed regularly to ensure that any new obligations and technologies, as well as any changes to our business operations and practices are taken into consideration, as well as that it remains abreast of the changing regulatory environment. Any personal information we hold will be governed by our most recent Privacy Notice.

If we decide to change our Privacy Notice, we will post those changes to this Privacy Notice and other places we deem appropriate.

## **16. Our products and services are not available to children**

Our products and services are not directed to persons under the age of 18, hereinafter "Children", "Child" and we do not knowingly collect personal information from Children. If we learn that we have inadvertently gathered personal information from a Child, we will take legally permissible measures to remove that information from our records. The Company will require the user to close his or her account and will not allow the use of our products and services. If you are a parent or guardian of a Child, and you become aware that a Child has provided personal information to us, please contact us at [support@kraken.com](mailto:support@kraken.com) and you may request to exercise your applicable access, rectification, cancellation, and/or objection rights.

## **17. Contact Information**

Any questions, complaints, comments and requests regarding this Privacy Notice are welcome and should be addressed to [support@kraken.com](mailto:support@kraken.com).

## **18. Data Protection Authorities**



If you are not satisfied with our response to your complaint, you have the right to submit a complaint with our regulator. You can contact the appropriate regulator direct from the details below:

**For residents of Australia:**

Office of the Australian Privacy Commissioner  
GPO Box 5218,  
Sydney, NSW 2001, Australia

**For residents of Canada:**

Office of the Privacy Commissioner of Canada  
30, Victoria Street  
Gatineau, QC K1A 1H3, Canada

**For residents of the United Kingdom:**

The Information Commissioner's Office  
Wycliffe House, Water Ln  
Wilmslow SK9 5AF, UK

**For residents of Europe:**

Irish Data Protection Commission  
21 Fitzwilliam Square South  
Dublin 2  
D02 RD28  
Ireland

**For residents of Japan:**

Personal Information Protection Commission  
Kasumigaseki Common Gate West Tower 32nd Floor,  
3-2-1, Kasumigaseki, Chiyoda-ku,  
Tokyo, 100-0013, Japan

**For clients of Kraken Futures (Singapore):**

Personal Data Protection Commission  
10 Pasir Panjang Road,  
#03-01 Mapletree Business City Singapore 117438

Take your cypto trading to the next level.

[Create account](#)

[Sign in](#)

## Features

[Buy Crypto](#)  
[Trade NFTs](#)  
[Trade Margin](#)  
[Trade Futures](#)  
[Institutions](#)  
[Security](#)  
[API Docs](#)  
[All features](#)

## Support

[Getting Started with Kraken](#)  
[Fund your Account](#)  
[Verify your Account](#)  
[Withdraw Cash](#)  
[Withdraw Crypto](#)  
[Visit Support Center](#)  
[Chat with Support](#)

## Crypto Prices

[Bitcoin Price](#)  
[Ethereum Price](#)  
[Ripple Price](#)  
[Cardano Price](#)  
[Solana Price](#)  
[Polygon Price](#)  
[All Crypto Prices](#)

## Company

[Create account](#)  
[Careers](#)  
[Blog](#)  
[Press](#)  
[Affiliate Program](#)  
[Status](#)

## Learn

[How to Buy Bitcoin](#)  
[Convert BTC to USD](#)  
[How to Buy Ethereum](#)  
[How to Buy Tether](#)  
[How to Buy Ripple](#)  
[How to Buy Cardano](#)  
[How to Buy Dogecoin](#)  
[How to Buy Monero](#)

## Community

© 2011 - 2023 Payward, Inc.

[Privacy Notice](#)  
[Terms of Service](#)  
[Cookies Policy](#)  
[Disclosures](#)

Language

U.S. English

*These materials are for general information purposes only and are not investment advice or a recommendation or solicitation to buy, sell or hold any cryptoasset or to engage in any specific trading strategy. Some crypto products and markets are unregulated, and you may not be protected by government compensation and/or regulatory protection schemes. The unpredictable nature of the cryptoasset markets can lead to loss of funds. Tax may be payable on any return and/or on any increase in the value of your cryptoassets and you should seek independent advice on your taxation position.*

